

Channel Impulse Response-based Distributed Physical Layer Authentication

Ammar Mahmood*, Waqas Aman*, M. Ozair Iqbal*, M. Mahboob Ur Rahman*, Qammer H. Abbasi†

*Electrical engineering department, Information Technology University (ITU), Lahore, Pakistan

{ammar.mahmood, waqas.aman, ozair.iqbal, mahboob.rahman}@itu.edu.pk

†Department of Electrical and Computer Engineering, Texas A&M University at Qatar
qammer.abbasi@qatar.tamu.edu

Abstract—In this preliminary work, we study the problem of *distributed authentication* in wireless networks. Specifically, we consider a system where multiple Bob (sensor) nodes listen to a channel and report their *correlated* measurements to a Fusion Center (FC) which makes the ultimate authentication decision. For the feature-based authentication at the FC, channel impulse response has been utilized as the device fingerprint. Additionally, the *correlated* measurements by the Bob nodes allow us to invoke Compressed sensing to significantly reduce the reporting overhead to the FC. Numerical results show that: i) the detection performance of the FC is superior to that of a single Bob-node, ii) compressed sensing leads to at least 20% overhead reduction on the reporting channel at the expense of a small (< 1 dB) SNR margin to achieve the same detection performance.

I. INTRODUCTION

Physical layer authentication addresses the problem of intrusion (impersonation) attack where a legitimate node Alice transmits its data to its intended recipient Bob, while Eve is an intruder node who unlawfully transmits on the channel allocated to Alice, in order to impersonate Alice before Bob. More precisely, for intrusion detection, Bob needs to authenticate each and every data packet it receives from the channel occupant (Alice or Eve). To carry out the (feature-based) authentication, Bob performs binary hypothesis testing while utilizing some device fingerprint (some physical layer attribute) as the decision metric.

The (authentication) problem at hand is in principle very similar to the classical problems of detection, classification, clustering etc. Nevertheless, the only important distinction is that in case of authentication problem, the device fingerprint of Eve is unknown. This limitation renders the classical likelihood ratio test (LRT) not computable (and hence Bayesian methods are not directly applicable). Therefore, Neyman-Pearson based binary hypothesis testing is typically implemented to carry out the authentication task at Bob.

As for the decision metric for binary hypothesis testing, Researchers have considered many different physical-layer attributes so far. Broadly speaking, these attributes can be classified into two categories: i) medium-based attributes, ii) hardware-based attributes. Medium-based attributes/fingerprints include different manifestations of the wireless channel such as channel frequency response [1],[2], channel impulse response [3],[4], received signal strength [5],

angle-of-arrival [6] etc. On the other hand, hardware-based attributes/fingerprints include carrier frequency offsets [7],[8], IQ-imbalance [9], mismatch parameters of non-reciprocal hardware [10] etc.

In this preliminary work, motivated by the classical distributed detection problem [11], we study the *distributed authentication* problem. Specifically, we consider a situation where instead of a single Bob (sensor) node, there are N Bob (sensor) nodes which all report their raw measurements or local decisions to a Fusion Center (FC) which makes the ultimate authentication decision. The need for Distributed Authentication arises whenever a single sensor (Bob) node alone can't be relied upon (e.g., it could come under deep fade/shadowing, it might have excessive AWGN/noise figure due to cheap receive circuitry etc.). Another potential application scenario is that of a Wireless Sensor Network [12] where the sensor (Bob) nodes are primitive in nature (i.e., they can't do sophisticated signal processing by themselves due to processor, storage and battery constraints); therefore, the sensor nodes simply relay the critical/sensitive data to the FC which carries out the ultimate authentication.

Contributions. The main contributions of this paper are the following: i) a preliminary study on distributed authentication, ii) exploitation of compressed sensing at the Bob nodes for significant reduction of the reporting overhead to the FC.

Outline. The rest of this paper is organized as follows. Section-II introduces the system model. Section-III provides the necessary background for the channel impulse response which has been utilized as device fingerprint in this work. Section-IV outlines the details of two strategies Bob (sensor) nodes could adopt to facilitate the cause of distributed detection. Section-V proposes to exploit compressed sensing at the Bob (sensor) nodes to reduce the overhead on the reporting channel. Section-VI provides some numerical results. Section VII concludes.

Notations. Bold-face letters (e.g., \mathbf{x}) represent vectors; Capitalized bold-face letters (e.g., \mathbf{X}) represent matrices; $\text{tr}(\cdot)$ denotes the trace operator; $(\cdot)^T$ denotes the transpose operator; $(\cdot)^H$ denotes the conjugate transpose operator; $\mathbb{E}(\cdot)$ denotes the expectation operator; *i.i.d* implies independent and identically distributed; $\mathbf{0}$ represents a vector (of appropriate length) of all zero's; $\text{blkdiag}(\mathbf{X}_1 \cdots \mathbf{X}_N)$ represents a block diagonal

matrix; $X \sim \mathcal{CN}(\cdot)$ signifies that X is a random variable with (circularly-symmetric) complex normal distribution; $\|\mathbf{x}\|_{l_p}$ represents the l_p -norm of vector \mathbf{x} .

II. SYSTEM MODEL

Following the spirits and motivation of distributed detection problem [11], this paper studies the distributed authentication problem whereby N number of Bob nodes simultaneously receive the packet sent by the channel occupant (either Alice or Eve) on the *sensing channel* (see Fig. 1). The N Bob nodes are either co-located (in the form of an antenna array), or, follow a random geometry (where each Bob node represents a different sensing device). In both scenarios, each Bob node reports some quantity (either its raw measurement, or, its local authentication decision) via a *reporting channel* to a Fusion Center (FC) which makes the ultimate authentication decision. Inline with previous literature [11], this work assumes that the reporting channel is error-free, delay-free and time-slotted (the performance curves obtained under these assumptions simply become upper-bounds on the performance curves obtained under realistic settings where these assumptions don't hold).

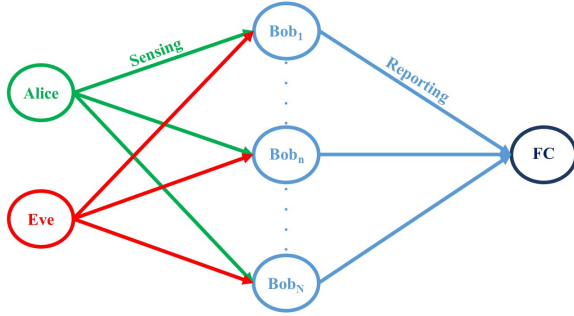


Fig. 1. The Distributed Authentication problem.

III. BACKGROUND: CHANNEL IMPULSE RESPONSE AS DEVICE FINGERPRINT

An intrusion (impersonation) attack occurs when an intruder node Eve unlawfully transmits on the (sensing) channel allocated to legitimate node Alice so as to impersonate Alice before Bob. To counter the challenge of intrusion attack, Bob needs to do authentication of each and every data packet it receives. Motivated by [4], this work utilizes the channel impulse response (CIR) as the device fingerprint for the purpose of authentication (at Bob nodes, or, Fusion center). More precisely, this work considers a single-carrier, wideband system with a time-slotted sensing channel (with τ seconds long timeslots). To introduce the notations, let's assume that Alice transmits on the shared sensing channel; then Bob n sees the channel $\mathbf{h}_{A,B_n}^{(i.i.d)}$. More precisely, $\mathbf{h}_{A,B_n}^{(i.i.d)}$ is the channel impulse response, i.e., $\mathbf{h}_{A,B_n}^{(i.i.d)} = [h_{A,B_n}(1) \ h_{A,B_n}(2) \ \dots \ h_{A,B_n}(L)]^T$ where $n = 1, \dots, N$ and L represents the total number of channel taps for the considered multipath (i.e., frequency-selective), time-invariant channel. Define:

$$\mathbf{H}_{AB}^{(i.i.d)} \triangleq [\mathbf{h}_{A,B_1}^{(i.i.d)} \ \mathbf{h}_{A,B_2}^{(i.i.d)} \ \dots \ \mathbf{h}_{A,B_N}^{(i.i.d)}] \in \mathbb{C}^{(L \times N)}$$

Typically, each of the columns of $\mathbf{H}_{AB}^{(i.i.d)}$ is modelled as a Complex Gaussian vector; moreover, all the columns (channel vectors) are considered to be *i.i.d*. However, in this study, we consider a more general/realistic setting; i.e., we assume that the channels measured by all the N Bob nodes are correlated (i.e., either all the Bob nodes are co-located, or, all the nodes in system model of Fig. 1 are located outdoors). Therefore, to make the columns of the matrix $\mathbf{H}_{AB}^{(i.i.d)}$ correlated with each other (to exploit the phenomena of compressed sensing later), we leverage the classical Kronecker-product based correlation model [13]. For the system model in Fig. 1, the Kronecker-product model reduces to the following:

$$\mathbf{H}_{AB} = \frac{1}{\sqrt{\text{tr}(\mathbf{R}_B)}} \mathbf{H}_{AB}^{(i.i.d)} \mathbf{R}_B^{1/2} \quad (1)$$

where $\mathbf{R}_B \in \mathbb{R}^{N \times N}$ represents the correlation matrix at the receive side (i.e., the correlation among Bob nodes). Specifically, we employ the exponential correlation model: $[\mathbf{R}_B]_{i,j} = \rho^{|i-j|}$ where $0 \leq \rho \leq 1$ is the correlation amount and i, j represent row and column indices of \mathbf{R}_B (or, Bob i and Bob j) respectively. Then, one can write: $\mathbf{H}_{AB} \triangleq [\mathbf{h}_{A,B_1} \ \mathbf{h}_{A,B_2} \ \dots \ \mathbf{h}_{A,B_N}]$.

Similarly, when Eve transmits on the shared sensing channel, then one can define:

$$\mathbf{H}_{EB}^{(i.i.d)} \triangleq [\mathbf{h}_{E,B_1}^{(i.i.d)} \ \mathbf{h}_{E,B_2}^{(i.i.d)} \ \dots \ \mathbf{h}_{E,B_N}^{(i.i.d)}] \in \mathbb{C}^{(L \times N)}$$

The channel matrix $\mathbf{H}_{EB} \triangleq [\mathbf{h}_{E,B_1} \ \mathbf{h}_{E,B_2} \ \dots \ \mathbf{h}_{E,B_N}]$ with correlated columns is then constructed via Eq. (1) as well¹.

IV. DISTRIBUTED AUTHENTICATION

This section outlines the proposed distributed authentication framework which in turn utilizes the channel impulse response as the transmit device fingerprint.

During m -th timeslot, either Alice, or, Eve will transmit on the sensing channel (assuming that Eve avoids collisions so as to stay undetected). Therefore, when Bob n receives a packet from the channel occupant (CO) (where $\text{CO} \in \{A, E\}$), it independently generates a measurement $\mathbf{z}_n(m)$ of its local CIR \mathbf{h}_{CO,B_n} as follows [4]:

$$\mathbf{z}_n(m) = \mathbf{h}_{CO,B_n} + \mathbf{v}_n(m) \quad (2)$$

where $\mathbf{v}_n(m)$ is the measurement noise. Specifically, $\mathbf{v}_n(m) \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma}_n)$ where $\mathbf{\Sigma}_n = \sigma_n^2 (\mathbf{S}^H \mathbf{S})^{-1} \in \mathbb{R}^{L \times L}$; σ_n^2 denotes the variance/power of the AWGN at Bob n . Furthermore, we assume that $\mathbf{v}_n(m)$ ($n = 1, \dots, N$) are *i.i.d*².

With the raw measurements of local CIR available at each Bob node, two distinct strategies are possible: i) each Bob node sends its raw measurement as is (along with the ground truth) to the FC, ii) each Bob node does the authentication locally and sends its binary decision to the FC. Both strategies are discussed below.

¹At this point, it is worth mentioning that we haven't incorporated the transmit side correlation (between Alice's antenna and Eve's antenna) into the Kronecker product model. The reason for this is that, inline with the previous work [1], we assume that Alice and Eve are spaced far apart (more than one wavelength) so that their mutual correlation is negligible.

² \mathbf{S} is the matrix formed by the training symbols. See [4] for more details.

A. Each Bob node sends its raw measurement as-is to the Fusion Center

Under this scenario, each Bob node sends its raw measurement \mathbf{z}_n as-is (along with the ground truth) to the FC³. Since an error-free, time-slotted reporting channel is assumed, FC receives all the (perfect) measurements after N time-slots (of the reporting channel). Fusion center then constructs a global measurement vector $\mathbf{z}_* \triangleq [\mathbf{z}_1^T \ \mathbf{z}_2^T \ \cdots \ \mathbf{z}_N^T]^T$. Then, we can write:

$$\mathbf{z}_* = \mathbf{h}_{\text{CO},\mathbf{B}*} + \mathbf{v}_* \quad (3)$$

where $\mathbf{h}_{\text{CO},\mathbf{B}*} \triangleq [\mathbf{h}_{\text{CO},B_1}^T \ \mathbf{h}_{\text{CO},B_2}^T \ \cdots \ \mathbf{h}_{\text{CO},B_N}^T]^T$ and $\mathbf{v}_* \triangleq [\mathbf{v}_1^T \ \mathbf{v}_2^T \ \cdots \ \mathbf{v}_N^T]^T$. \mathbf{v}_* represents the global estimation error; $\mathbf{v}_* \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma}_*)$ where $\mathbf{\Sigma}_* = \text{blkdiag}(\mathbf{\Sigma}_1 \ \mathbf{\Sigma}_2 \ \cdots \ \mathbf{\Sigma}_N) \in \mathbb{R}^{(L \times N) \times (L \times N)}$.

With \mathbf{z}_* available, the FC casts the sender-node authentication problem as a binary hypothesis testing problem:

$$\begin{cases} H_0 : \mathbf{z}_* = \mathbf{h}_{\text{AB}*} + \mathbf{v}_* \\ H_1 : \mathbf{z}_* = \mathbf{h}_{\text{EB}*} + \mathbf{v}_* \end{cases} \quad (4)$$

where $\mathbf{h}_{\text{AB}*} = [\mathbf{h}_{A,B_1}^T, \mathbf{h}_{A,B_2}^T, \dots, \mathbf{h}_{A,B_N}^T]^T$ and $\mathbf{h}_{\text{EB}*} = [\mathbf{h}_{E,B_1}^T, \mathbf{h}_{E,B_2}^T, \dots, \mathbf{h}_{E,B_N}^T]^T$. Then, $\mathbf{z}_*|H_0 \sim \mathcal{CN}(\mathbf{h}_{\text{AB}*}, \mathbf{\Sigma}_*)$ and $\mathbf{z}_*|H_1 \sim \mathcal{CN}(\mathbf{h}_{\text{EB}*}, \mathbf{\Sigma}_*)$. If $H_0 = 1$, received data (on the sensing channel) is accepted by the FC; if $H_1 = 1$, received data is discarded by the FC.

Next, assuming that $\mathbf{h}_{\text{AB}*}$ is known to the FC (via the prior training of the Bob nodes, on a secure channel) with sufficient accuracy, the FC applies the following test [4]:

$$(\mathbf{z}_* - \mathbf{h}_{\text{AB}*})^H \mathbf{\Sigma}_*^{-1} (\mathbf{z}_* - \mathbf{h}_{\text{AB}*}) \underset{H_0}{\overset{H_1}{\gtrless}} \delta \quad (5)$$

where δ is the comparison threshold whose value is to be determined by the FC. This work follows Neyman-Pearson procedure to systematically compute the threshold δ . Specifically, δ is computed from a pre-specified, maximum Type-1 error (i.e., probability of false alarm, P_{fa}) that the FC can tolerate. Then, for a given Type-1 error, Neyman-Pearson method guarantees to minimize the Type-2 error (i.e., probability of missed detection, P_{md}).

Denote by T the test statistic in Eq. (5); i.e., $T = (\mathbf{z}_* - \mathbf{h}_{\text{AB}*})^H \mathbf{\Sigma}_*^{-1} (\mathbf{z}_* - \mathbf{h}_{\text{AB}*})$. Then, the test statistic $T|H_0 \sim \chi^2(2NL)$; i.e., T has central Chi-squared distribution with $2NL$ degrees of freedom, under H_0 . Then, the probability of false alarm P_{fa} (i.e., incorrectly identifying Alice's packet as if it is from Eve) is given as:

$$P_{fa} = \Pr(T > \delta | H_0) = \int_{\delta}^{\infty} p_{T|H_0}(x) dx \quad (6)$$

where $p_{T|H_0}(x) \sim \chi^2(2NL)$ is the probability density function of $T|H_0$. Thus, one can set P_{fa} to some value α in Eq. (6) and solve for the threshold δ .

With $P_{fa} = \alpha$, the performance of the hypothesis test in Eq. (5) is solely characterized by the Type-2 error a.k.a the

probability of missed detection: $P_{md} = \Pr(T < \delta | H_1)$. Since computing the distribution of $T|H_1$ is quite involved, we numerically compute the value of P_{md} in simulation section.

B. Each Bob node sends its local decision to the Fusion Center

Under this scenario, Bob node n (independently) utilizes its measurement \mathbf{z}_n of its local CIR $\mathbf{h}_{\text{CO},B_n}$ (see Eq. (2)) to construct the following binary hypothesis testing problem:

$$\begin{cases} H_0 : \mathbf{z}_n = \mathbf{h}_{A,B_n} + \mathbf{v}_n \\ H_1 : \mathbf{z}_n = \mathbf{h}_{E,B_n} + \mathbf{v}_n \end{cases} \quad (7)$$

Once again, assuming that \mathbf{h}_{A,B_n} is perfectly known to Bob n , it applies the following test [4]:

$$(\mathbf{z}_n - \mathbf{h}_{A,B_n})^H \mathbf{\Sigma}_n^{-1} (\mathbf{z}_n - \mathbf{h}_{A,B_n}) \underset{H_0}{\overset{H_1}{\gtrless}} \delta_n \quad (8)$$

where δ_n is the comparison threshold whose value is to be determined by Bob n . Once again, we follow the Neyman-Pearson procedure to systematically compute the threshold δ_n .

Denote by T_n the test statistic in Eq. (8); i.e., $T_n = (\mathbf{z}_n - \mathbf{h}_{A,B_n})^H \mathbf{\Sigma}_n^{-1} (\mathbf{z}_n - \mathbf{h}_{A,B_n})$. Then, the test statistic $T_n|H_0 \sim \chi^2(2L)$; i.e., T_n has central Chi-squared distribution with $2L$ degrees of freedom, under H_0 . Then, the probability of false alarm $P_{fa,n}$ is given as:

$$P_{fa,n} = \Pr(T_n > \delta_n | H_0) = \int_{\delta_n}^{\infty} p_{T_n|H_0}(x) dx \quad (9)$$

where $p_{T_n|H_0}(x) \sim \chi^2(2L)$ is the probability density function of $T_n|H_0$. Thus, one can set $P_{fa,n}$ to some value α_n in Eq. (9) and solve for the threshold δ_n .

With $P_{fa,n} = \alpha_n$, the performance of the hypothesis test in Eq. (8) is solely characterized by the Type-2 error a.k.a the probability of missed detection: $P_{md,n} = \Pr(T_n < \delta_n | H_1)$. Since it is difficult to compute the distribution of $T_n|H_1$, we numerically compute the value of $P_{md,n}$ in simulation section.

Then, the Fusion Center, having received the vector of local (binary-valued, hard) decisions \mathbf{u}_* by all the Bob nodes, applies the following (heuristic) fusion rules to generate the ultimate (binary-valued, hard) decision: i) OR (optimistic) rule, ii) AND (pessimistic) rule, iii) majority voting, iv) weighted averaging.

V. OVERHEAD REDUCTION ON REPORTING CHANNEL VIA COMPRESSED SENSING

This section attempts to invoke Compressed Sensing⁴ at the Bob nodes owing to the fact that the CIR measurements made by the Bob nodes are correlated (see Eq. 1). To this end, this section focuses on a specialized system model (more than the one given in Fig. 1 earlier) whereby the N (N is large) Bob nodes are all co-located as a linear antenna-array on a single receive device, now-called the relay node. Such system model could represent, for example, a situation where a

³For clarity of exposition, we drop the time-slot index m in the rest of this paper.

⁴The interested reader is referred to [14] for a comprehensive overview of compressed sensing.

multi-antenna relay node (e.g., a massive MIMO base station) forwards the data of a source (with unknown identity) towards a destination (the FC). Moreover, the relay node can either stay indifferent/blind to the authentication cause of the FC (the raw measurements case), or, the relay node could help the authentication cause of the FC (the local decisions case). We further assume that the relay node doesn't know its (vector) channel towards the FC. Thus, the multi-antenna relay doesn't do beamforming towards the FC; it rather transmits the length- NL vector (containing raw measurements or local decisions) to the FC in a sequential manner. All in all, this specialized system model allows us to invoke compressed sensing (CS) at the relay node (to compress the length- NL report vector into a length- M vector where $M \ll NL$) to reduce the number of channel uses (from N to M) on the reporting channel.

At this point, it is worth mentioning that to exploit compressed sensing under the generalized system model shown in Fig. 1, one needs to employ more sophisticated medium access schemes on the reporting channel (which is beyond the scope of the current work)⁵.

We now recall from the previous section that having received the data from the (sensing) channel occupant (Alice or Eve), the relay node could adapt either of the two distinct *compress-and-forward* strategies: i) the relay node compresses the vector of raw measurements and sends it to the FC (along with the vector of ground truths), ii) the relay node compresses the vector of local decisions and sends it to the FC. Both strategies are discussed below.

A. The relay node compresses the vector of raw measurements and sends it to the Fusion Center

The relay node compresses the vector of raw measurements $\mathbf{z}_* \in \mathbb{C}^{(NL \times 1)}$ (see Eq. 3) into a vector $\mathbf{y} \in \mathbb{C}^{(M \times 1)}$ ($M \ll NL$) via random projections method:

$$\mathbf{y} = \Phi \mathbf{z}_* \quad (10)$$

where $\Phi \in \mathbb{R}^{(M \times NL)}$ is a random matrix, the so-called sensing/measurement matrix, whose entries are typically the realizations of *i.i.d* Gaussian or Bernoulli variables.

After the compression, the relay node transmits the vector \mathbf{y} to the FC in M time-slots. Due to the error-free reporting channel, the FC receives \mathbf{y} as-is; therefore, its task becomes to recover an estimate $\hat{\mathbf{z}}_*$ of \mathbf{z}_* from \mathbf{y} . To this end, we invoke the classical Orthogonal Matching Pursuit (OMP) algorithm at the FC [16]. Specifically, the OMP solves the following l_1 -norm minimization problem:

$$\min \|\mathbf{z}_0\|_{l_1} \text{ s.t. } \mathbf{y} = \Phi \Psi^T \mathbf{z}_0 \quad (11)$$

where

$$\mathbf{z}_0 = \Psi \mathbf{z}_* \quad (12)$$

is the actual K -sparse representation of \mathbf{z}_* in a transform domain. The matrix Ψ is called the sparsifying basis. The most

frequently used sparsifying basis Ψ include discrete Fourier transform (DFT), discrete cosine transform (DCT), Karhunen-Loeve Transform (KLT) etc. Finally, when $\hat{\mathbf{z}}_*$ is available via Eqs. (11),(12), the FC follows the procedure of Section-IV-A to carry out the authentication.

At this point, it is necessary to emphasize that the invocation of compressing sensing at the relay node is feasible only when the vector \mathbf{z}_* is K -sparse (for some $K \ll NL$) in some transform domain. This condition is fulfilled when the channel under consideration exhibits spatial correlation (see Eq. 1) [17]. Typically, the reconstruction error $\mathcal{E} = \mathbb{E}[\|\hat{\mathbf{z}}_* - \mathbf{z}_*\|_{l_2}^2]$ decreases with increase in ρ (see Eq. 1) and vice versa.

B. The relay node compresses the vector of local decisions and sends it to the Fusion Center

Under this strategy, the relay node compresses the vector of local decisions $\mathbf{u}_* \in \{0,1\}^{(NL \times 1)}$ into a vector $\mathbf{y} \in \{0,1\}^{(M \times 1)}$ ($M \ll NL$) via random projections method and transmits \mathbf{y} to the FC in M time-slots, as discussed above. The FC then recovers $\hat{\mathbf{u}}_*$ from \mathbf{y} via OMP and follows the procedure of Section-IV-B to carry out the authentication task.

VI. NUMERICAL RESULTS

We assume uniform power delay profile (PDP) to generate each of the N CIRs (with $L = 6$ taps each) on the sensing channel. The received SNR at Bob n is defined as $1/\sigma_n^2$ where σ_n^2 is the power of AWGN at Bob n . Furthermore, we evaluate the case of homogeneous SNRs only (i.e., we assume that the SNR/link quality of all the N sensing links is the same). Finally, in all the results below, we evaluate the detection probability P_d (where $P_d = 1 - P_{md}$) of the FC as the SNR (of a single sensing link) is varied over its full operational range.

Fig. 2 represents the case when Bob nodes send their Raw Measurements to the FC. For Fig. 2, we set $N = 10$; the threshold δ is varied over the range: 260 : 20 : 340. Fig. 2 shows that with decrease in δ (or, equivalently, with increase in the false alarm rate P_{fa}), the detection probability increases as one would intuitively expect. Additionally, the detection performance remains stable to a high value (close to 1) for SNR (at the FC) as low as 5 dB.

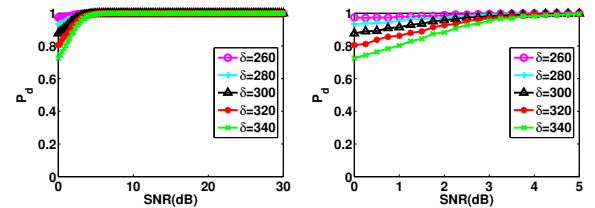


Fig. 2. Detection performance of the FC when Bob nodes send their Raw Measurements to FC (right-side plot shows the zoomed-in view (corresponding to $\text{SNR} \in 0 - 5$ dB) of the left-side plot).

Fig. 3 represents the case when Bob nodes send their Local Decisions to FC. In Fig. 3, $N = 10$; additionally, from top to bottom, each of the N thresholds is varied as: $\delta_n \in \{39, 32.9, 26.2\}$ which maps to the false alarm rates:

⁵For example, [15] presents a scheme where during each of the M time-slots, each of the N sensor nodes transmits its local measurement to the FC with some probability p , thus making the sensing/measurement matrix Φ non-Gaussian.

$P_{fa,n} \in \{0.0001, 0.001, 0.01\}$ respectively. Fig. 3 shows that the AND-ing (OR-ing) based pessimistic (optimistic) fusion rule performs the best (worst) while the performance of the Majority Voting (Averaging) fusion rule is slightly better than (same as) the performance achieved by a single Bob node. Additionally, from top to bottom, sacrifice in terms of more and more false alarm rate results in improvement of detection performance of all the schemes for any given SNR.

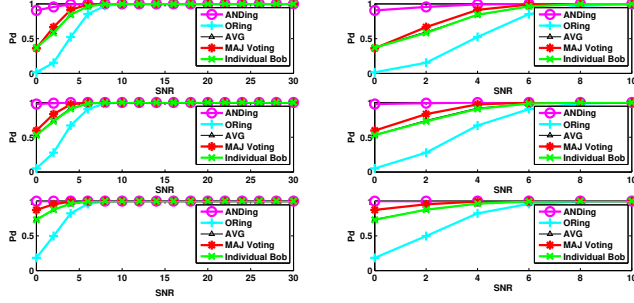


Fig. 3. Bob nodes send their Local Decisions to the FC (right-side plot shows the zoomed-in view (corresponding to SNR $\in 0 - 10$ dB) of the left-side plot).

Figs. 4, 5 show the results equivalent to Figs 2, 3 when the Bob nodes (a.k.a the relay node) invoke the compressed sensing before sending their measurements to the FC. For compressed sensing, we have used a Gaussian measurement matrix Φ and DCT as the sparsifying basis Ψ .

Fig. 4 represents the case when Bob nodes send their raw measurements to the FC after compressed sensing. In Fig. 4, we set $N = 100$; the threshold δ is varied in the range: $\delta \in \{2600, 4800, 5000\}$. The compressed sensing compresses the length $N \times L = 100 \times 6 = 600$ measurement vector \mathbf{z}_* into a length $M = 480$ vector achieving a saving of 20% in reporting overhead. Fig. 4 basically compares the two strategies by the relay node: S1) the relay node does the CS prior to sending the raw measurement vector to the FC, S2) the relay node sends the raw measurement vector as-is to the FC. Fig. 4 indicates that a small (< 1 dB) SNR margin is needed by S1 to achieve the same detection performance as S2, due to finite reconstruction error \mathcal{E} at the FC.

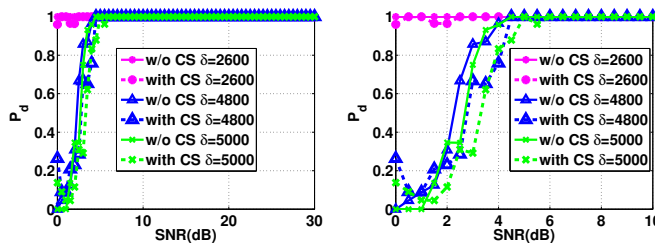


Fig. 4. Bob nodes send their raw measurements to the FC via compressed sensing (right-side plot shows the zoomed-in view (corresponding to SNR $\in 0 - 10$ dB) of the left-side plot).

Fig. 5 represents the case when Bob nodes send their local decisions to the FC after compressed sensing. In Fig. 5, we

set $N = 100$; additionally, from top to bottom, each of the N thresholds δ_n is varied in the range: $\delta_n \in \{39, 32.9, 26.2\}$ which maps to the following false alarm rates: $P_{fa,n} \in \{0.0001, 0.001, 0.01\}$ respectively. In all the three plots, the performance of the majority voting based fusion rule is considered with and without compressed sensing at the Bob nodes. In this case, compressed sensing at the Bob nodes leads to a 30% overhead reduction on the reporting channel.

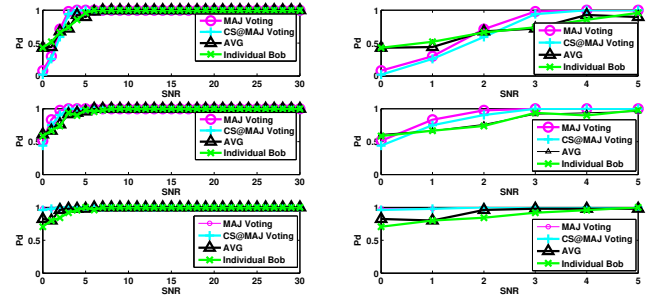


Fig. 5. Bob nodes send their local decisions to the FC via compressed sensing (right-side plot shows the zoomed-in view (corresponding to SNR $\in 0 - 5$ dB) of the left-side plot).

VII. CONCLUSION

We did a preliminary study on the problem of distributed authentication in wireless networks. Specifically, we considered a system where multiple Bob (sensor) nodes listen to a channel and report their *correlated* measurements to a Fusion Center (FC). Numerical results showed that the authentication performance of the FC is superior to that of a single Bob node. Additionally, the correlated measurements by the Bob nodes allowed us to invoke compressed sensing at the Bob nodes to reduce the reporting overhead to the FC by at least 20%. Immediate future work will investigate the design of: i) optimal decision rules at the Bob nodes and the FC, ii) clever medium access schemes on the reporting channel.

ACKNOWLEDGEMENTS

This publication was made possible by NPRP grant #7 - 125-2-061 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

REFERENCES

- [1] L. Xiao, L. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571-2579, July 2008.
- [2] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over mimo fading wiretap channels," *IEEE Transactions on Wireless Communications*, vol. 11, no. 7, pp. 2564-2573, July 2012.
- [3] F. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. of IEEE MILITARY COMMUNICATIONS CONFERENCE, (MILCOM)*, Nov 2011, pp. 538-542.
- [4] J. Tugnait and H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," in *Proc. of Second*

International Conference on Communication Systems and Networks (COMSNETS), Jan 2010, pp. 1–9.

- [5] J. Yang, Y. Chen, W. Trappe, and J. Cheng, “Detection and localization of multiple spoofing attackers in wireless networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 44–58, Jan 2013.
- [6] J. Xiong and K. Jamieson, “Secureangle: Improving wireless security using angle-of-arrival information,” in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, ser. Hotnets-IX. New York, NY, USA: ACM, 2010, pp. 11:1–11:6. [Online]. Available: <http://doi.acm.org/10.1145/1868447.1868458>
- [7] W. Hou, X. Wang, and J. Chouinard, “Physical layer authentication in ofdm systems based on hypothesis testing of cfo estimates,” in *Proc. of IEEE International Conference on Communications (ICC)*, 2012, pp. 3559–3563.
- [8] M. Ur Rahman, A. Yasmeen, and J. Gross, “Phy layer authentication via drifting oscillators,” in *Global Communications Conference (GLOBECOM)*, 2014 IEEE, Dec 2014, pp. 716–721.
- [9] P. Hao, X. Wang, and A. Behnad, “Performance enhancement of i/q imbalance based wireless device authentication through collaboration of multiple receivers,” in *2014 IEEE International Conference on Communications (ICC)*, June 2014, pp. 939–944.
- [10] M. M. U. Rahman and A. Yasmeen, “Exploiting lack of hardware reciprocity for sender-node authentication at the phy layer,” *arXiv preprint arXiv:1610.02658*, 2016.
- [11] R. Viswanathan and P. K. Varshney, “Distributed detection with multiple sensors i. fundamentals,” *Proceedings of the IEEE*, vol. 85, no. 1, pp. 54–63, Jan 1997.
- [12] K. Bauer and H. Lee, “A distributed authentication scheme for a wireless sensing system,” *ACM Transactions on Information and System Security*, vol. 11, no. 3, pp. 1–35, 2008.
- [13] J. P. Kermoal, L. Schumacher, K. I. Pedersen, P. E. Mogensen, and F. Frederiksen, “A stochastic mimo radio channel model with experimental validation,” *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 6, pp. 1211–1226, Aug 2002.
- [14] E. J. Candès and M. B. Wakin, “An introduction to compressive sampling,” *IEEE signal processing magazine*, vol. 25, no. 2, pp. 21–30, 2008.
- [15] G. Yang, V. Y. Tan, C. K. Ho, S. H. Ting, and Y. L. Guan, “Wireless compressive sensing for energy harvesting sensor nodes,” *IEEE Transactions on Signal Processing*, vol. 61, no. 18, pp. 4491–4505, 2013.
- [16] J. A. Tropp and A. C. Gilbert, “Signal recovery from random measurements via orthogonal matching pursuit,” *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4655–4666, Dec 2007.
- [17] P. H. Kuo, H. T. Kung, and P. A. Ting, “Compressive sensing based channel feedback protocols for spatially-correlated massive antenna arrays,” in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2012, pp. 492–497.